(51) International Patent Classification 6 : G07D 7/00	A1	(11) International Publication Number: WO 99/27503
		(43) International Publication Date: 3 June 1999 (03.06.99)

(54) Title: THE SYSTEM AND METHOD OF PROTECTION AND HANDLING OF DOCUMENTS

(57) Abstract

The solution deals with a system for the protection of physical documents against illegal and unauthorized alteration, modification or counterfeiting, and allowing for falsification–proof confirmation of the inspection of the document, and minimizing the influence of the human factor. The system consists of at least one document generation block (300), creating from the document data source (200) with the involvement of an operator (800) and/or (801) the physical form of the document. The system also includes the crypto mark (400) carried by the document which then becomes a component part of the shadow document database (101); at least one document control block (500) which scans the crypto mark (400) carried by the document, verifies its authenticity, displays the critical part of the document and generates the crypto stamp (900). The crypto stamp is affixed either by the authorized operator (800) and/or (801) or an appropriate equipment onto the document which thus becomes a component part of the feedback document database (503); at least one keys generation and distribution block (700); at least one document database comparison block (600); and at least one document source block (200). The solution also deals with the method of protection of physical documents, which consists of cryptographic processing of the selected data at the point of the creation of the document, and transformation of the data into a form serving as a base for the generation of the crypto mark; the system includes also the generation of the crypto mark and its scanning at the point where the inspection of the document takes place and transformation into a data form followed by verification of integrity and validity of those data and approval of the document inspection; the final step consists of the generation and displaying of the crypto stamp and its affixing onto the inspected document for its further use.
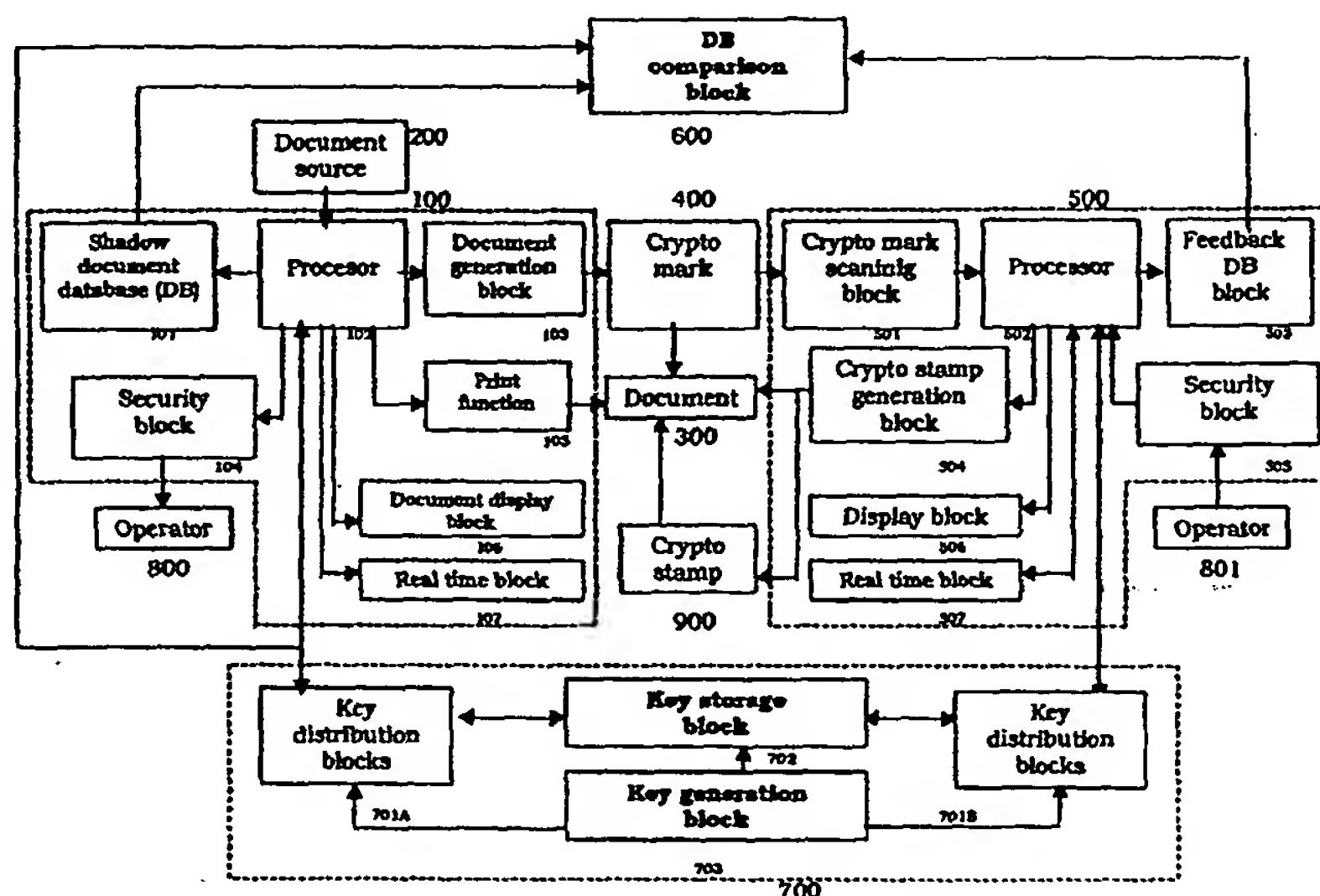
FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

The system and method of protection and handling of documents

Technical Field

The invention relates to the system and method of protection of integrity of printed documents, and to prevention of their unauthorized modification, counterfeiting and performing of related activities, as well as to minimizing of the influence of the human factor.

Beckground Art

The literature describes several ways of the protection of documents, all of which are aimed at the protection and encryption of documents and the prevention of their unauthorized modification and counterfeiting. Considering the system and mode of the protection, there are three basic concepts.

The first of them deals with the protection of a document as such (i.e. checks, various types of identification documents). This group of documents carries protective marks including e.g. a protective type of paper they are made from, ink and fibers sensitive to ultraviolet light, pantographs, artificial water-marks, embossing, etc. Numerous reports deal with the protection of checks and other documents, e.g. deeds of donation, motor vehicle identification documents and certificates of titles, airline tickets, school diplomas, various admission tickets, securities, bonds, certified copies of school certificates and various types of legal documents, etc. The system involves e.g. protective inks either indicating that the document has been altered or enabling the verification of the original copy (deletable inks, fluorescent inks, infra-red inks, inks penetrating into the depth of the paper the document is printed on, thermochromic inks, chemically reactive types of paper, protective fibers, water-marks, etc. (Copyright 1996 FORM magazine, 433 - E. Monroe Avenue, Alexandria, VA 22301). Apart from water-marks and fluorescent ink, the systems very often utilize also the photomicrograph. This group of "hidden marks" represents an effective deterring means offering an efficient protection against copying and scanning of documents. In order to achieve maximum protecting effect, the documents belonging into this group should include several marks (e.g. some types of recently used checks carry up to 16 anti-criminal marks). Other often used modes of protection utilize various printing techniques such as multicolor prismatic printing, holographic printing, foil embossing, etc.

The second concept is based on the protection of the content of the documents (i.e. of the data incorporated into the given document). EP 0084441 A2 830727, for example, deals with the mode and technology used for the protection of computer software against unauthorized use. This class of protection methods is the most numerous one and more examples shall be given in the text below.

The protection of the "uniqueness" of the document, i.e. of the document the content and base of which cannot be duplicated, represents the most elaborate way of protection, and methods representing the combination of the preceding two concepts are available at the time being.

The area of the protection of documents and of their handling involves solutions ensuring certain partial aspects of the protection, such as:

Protection of the base of the document through different printing, graphic and paper production technology-related elements. Other systems may involve chemical, optical, electromagnetic and similar protective elements representing an effective barrier to the illegal

- 2 -

production of the protected documents (bills, checks, bonds, securities, admission tickets, etc.).

Protection against duplication of documents, e.g. through creation of a special graphic mark(s) as an integral part of the document. Specially equipped copiers (available at specialized workplaces) shall recognize such mark(s) and shall thus refuse to copy the document (US Patent No. 5502575).

Protection supplemented with an active element making it possible to transport on the document a protective mark able to activate the appropriate equipment (copier, fax) which in turn will carry out the instruction (US Patent No. 5231663).

Elements carried either in the text of the document or in the document as such, providing for the automated handling of printed documents through marks representing either numbers or other types of information required for the appropriate classification of the document (name of the author, title, serial number, date, etc.). These marks may be in the form of bar codes or information included directly into the base of the document (US Patents Nos. 5490217 and 5486686, respectively).

Yet another group of relevant technologies is represented by techniques used for the inclusion of certain protective information into a document printed on paper:

Methods making it possible to print through various graphic combinations on certain places, designated for that purpose within the document, scannable data either in the form of double-value surface information (US Patent No. 5337362) or as more complex and intricate two-dimensional (2D) bar codes (e.g. US Patent No. 5243655), or by sophisticated optical cryptographic methods (US Patent No. 5488664) belonging into the group of the so called 'water-marks' (analogous to classical water-marks). Other methods include rather complex encrypting techniques (data embedding) and advanced methods based on hidden information included directly into the base of the document (watermarking) which are not visible and/or legible to the naked eye (e.g. US Patent No. 5629770). However, information included into the document in this way is rather limited (serial number of the document, copyright-related data, originator of the document [person or software], etc.).

The third group is represented by technologies protecting either a certain form of the contents of the document - e.g. its scanned/printed form (including fax) - or a part of a document which is in data form, with the aim to authenticate both the document and its contents. However, the protective mark does not allow for the determination of the data form of the document or of its part. This type of protection is represented by various authentication methods based on signature, and is used in the case of electronic form of documents (e.g. US Patents Nos. 5530755, 5255106, 5388158, 5157726).

The authentication of the document (of its scanned graphic version) will be carried out at the document inspection/use point, verifying thus the integrity/intactness of the content of the document. However, the document itself - in the data form - remains inactive.

A specific category of technologies is represented by techniques protecting through partially cryptographical methods the content of a document in its printed bitmap form. After encryption (also scrambling), a signature will be created and printed at the sending side. At the receiving side, the document will be decrypted (descrambled) and the correctness/authenticity of the signature will be checked. This category allows for direct protection of the contents of the document, regardless of its original data form (e.g. US Patents Nos. 5321749, 5491536).

However, the available literature does not describe any solution utilizing cryptographic tools for the creation of a broad system that would provide comprehensive protection of the document and, at the same time, of the activities associated with its handling, and that would be based on protected feed-back information from the critical

points of the movement (and/or functions) of the document. However, such a solution represents the subject of the present invention.

Disclosure of the Invention

The method and the system of the protection of printed documents and operations related to their use are based on the generation of falsification-proof and non-alterable ways of information transfer within the variable environment of the system as a whole. Within this environment, the information which is in an electronic form is being transformed into a printed document (hard copy). Another important aspects of this invention are the exclusion of the human factor from all critical operations, and the introduction of an effective and falsification-proof feedback from the critical operations themselves as well as from the points where these critical operations are being effected (places of the creation and inspection of the document).

The subject of the invention is a system designated for the protection of physical documents against illegal and unauthorized modification or counterfeiting, and allowing for falsification-proof confirmation of the inspection of the document and minimizing of the influence of the human factor. The system consists of:

— at least one document generation block, creating from the data source and with the involvement of an authorized operator the physical form of the document, a crypto-mark carried by the document, and a shadow document database;

— at least one document inspection block, scanning and verifying the authenticity of the crypto mark carried by the document, displaying the critical parts of the document, generating the crypto stamp to be placed by an authorized operator or equipment onto the document, and creating the feedback document database;

— at least one key generation and distribution block;

— at least one document database comparison block;

— at least one document source block.

The document generation block consists of a processor, carrying out the data processing and containing the crypto keys, a document printing block, a crypto mark generation block, a safety block, a real time block, a displaying block, and a shadow document database generating block.

The document inspection block consists of a processor carrying out the data processing and containing the crypto keys, a document printing block, a crypto mark scanning block, a safety block, a real time block, displaying block, a shadow document database generating block, and a crypto stamp generation block.

The key generation and distribution block consists of a generating block, a key storage block, and a key distribution block.

The database comparison block consists of a comparison and evaluation block, a comparison conditions block, an alarm and warning generating block, and a statistical summaries block.

- 4-

The subject of the invention includes also the method of protection of physical document against their illegal and unauthorized modification and counterfeiting, and allowing for falsification-proof confirmation of the inspection of the document and minimizing of the influence of the human factor. The system consists of:

— cryptographic processing of the selected data which is carried out at the place of the generation of the document and which is the source of the data required for the printing of this physical printed document, as well as transforming of the data into a form representing the basis for the generation of the crypto mark;

— generating of the crypto mark by the equipment designated for that purpose, which takes place after the transformation of the data cryptographically processed for the purpose of the crypto mark generation; the crypto mark thus generated becomes unseparated part of the physical document which thus becomes its carrier transferring the crypto mark to the place(s) of the use of the document;

— scanning of the crypto mark at the document inspection verification point and its transformation into a data form;

— the use of cryptographic methods for the verification -- based on the scanned crypto mark -- of the integrity and validity of the data;

— approval by an authorized operator of the inspection of the document and of the associated activities, carried out after the completion of the inspection;

— generation, and displaying of the crypto stamp linking unambiguously the controlled document to the place and exact time of the inspection carried out by an authorized operator;

— affixing of the crypto stamp onto the controlled document for the purpose of its further use by an authorized operator either in a manual way or with the use of an appropriate equipment.

The subject of the invention includes also the collecting at the point of the generation of the document of all document thus created, their equipment with electronic signature and dispatching either individually or in batches in the encrypted (protected) form as a shadow database into the database comparison block.

All documents that have passed the inspection step shall be gradually accumulated at the document inspection point where they shall be electronically signed and dispatched either individually or in batches in an encrypted (protected) form as a feedback database into the database comparison block.

The crypto mark thus generated, if it is in the form of an individual physical object (e.g. sticker, annex, supplement, etc.), shall be permanently attached to the document.

The crypto mark - if generated in the same way as the document - becomes unseparated part thereof printed (in the form of a bar code or a chain of OCR symbols) on the part of the surface of the carrier material (e.g. paper) designated for that purpose.

The crypto mark thus generated may be embedded either into the text of the document and/or into its graphical part (e.g. through watermarking, etc.) or into the printing background of the document.

- 5-

The DB comparison block performs the comparison of the database operations over the contents of the shadow DB and feedback DB.

Based on the data scanned from the crypto mark and data received from the point of the inspection of the document, the crypto stamp generation block located at the document inspection point will generate a crypto stamp, by cryptographic operation.

In the step that follows, the crypto stamp will be either placed, affixed onto or coupled with the document.

The key generation block will create the encryption and decryption keys which will be distributed by the key distribution block through safe channel(s) into the document generation and document control blocks.

The operator will then perform the operation related to the verification of his/her authorization to carry out the given set of activities, performed against the document generation block through the security block.

In the next step, the operator will then perform the operation related to the verification of his/her authorization to carry out the given set of activities, performed against the document inspection block through the safety block.

Finally, the operator will perform the verification of his/her identity and authorization to carry out certain activities involving the use of the document generation and inspection blocks.

The invention provides solution for the generation of a structure involving safe transfer channels between the document generation, document inspection, key generation and distribution, document database comparison, and document source blocks and determining the relationships of those blocks with the printed document and the crypto mark attached to it, and also with the crypto stamp. The invention introduces into one of the most critical activity, i.e. into the procedure of the inspection of the document, at least two operations contributing significantly to the enhancement of both the safety of that activity and the future auditing of the document. Those two operations are the machine-mediated transfer of the contents of the document, or of its most important parts, from the crypto mark, and the transfer of the scanned information into the computer. The computer verifies the authenticity and integrity of the document and generates its original/authentic and true form. As a further step, the computer generates a crypto stamp. The crypto stamp, that is being affixed (either printed or hand-written) onto the document, serves as an undeniable proof that the operator has carried out the required control activity.

Of great importance is also the fact that the document, together with the crypto stamp affixed to it, represents a communication channel characterized by a high degree of availability.

Another important aspect of the invention is the closure of a inspection feedback between the place(s) of generation and inspection of the document, which is effected in the DB comparison block, and which represents a cryptographic and safe closure of all activities

directly associated with the cycle consisting of the generation, transport, and inspection of the document.

The security aspect of the invention is further enhanced by the activities effected within the security block which are aimed at safe determination of the authorization of a given operator to carry out activities associated with the generation/creation and inspection of the document.

Similarly, the key generation and distribution block carries out safety operations resulting in cryptographically safe generation of keys, their storage, and safe distribution to the points of their use.

Brief Description of Drawings

Figure 1 shows all of the above mentioned blocks which represent the principal components of the invention, and their mutual interconnection and/or functional relationships. Figure 2 shows the DB comparison block.

Best Mode for Carrying Out the Invention

Example 1

The system as a whole represents a safe and functional environment enabling the creation of a critical document 300. The document is generated in the document source 200 which itself is located within the document generation block 100. The crypto mark 400 may be affixed onto a document either at the time of its generation or later.

Document 300 with the crypto mark 400 affixed to it is transferred to the document inspection point that is located within the document inspection block 500. Both blocks are connected through a safe and authenticated way with an operator 800 (and/or 801).

At the inspection point, which is located at the document inspection block 500, the operator 801 verifies his/her authorization to perform the inspection operations. Having scanned the crypto mark 400 from the document 300, the document control block 500 carries out a cryptographic verification of the integrity of the document 300 and displays its electronic form. Operator 801 makes a decision regarding the conclusion of the document control and enters the corresponding command into block 500. The document control block 500 generates through a cryptological method a crypto stamp 900, which will be displayed and either manually attached or directly printed onto the document 400.

The generation of a document in the document generation block 100 is either accompanied or followed by the generation of a cryptographically protected shadow document database (DB) 101. The document is stored in the shadow DB 101 and sent in an encrypted and protected form into the DB comparison block 600.

In a similar way, upon inspecting the document 300 in the inspection block 500, the feedback DB block 503 creates a cryptographically protected database of inspected documents and the electronic form of the document is saved and sent in a protected and encrypted form into the DB comparison block 600.

The key element of the document generation block 100 is the processor 102 integrating within the document generation block 100 the (program) functions of other blocks.

The crypto mark generation block 103 which may be realized either as an independent block or as a software function within the processor block 102 generates through its cryptographic function a crypto mark that will be subsequently printed onto the document 300.

The document itself will be created either independently from the crypto mark through the print function 105 or within a single united technological step.

The document generation block contains the document display block 106 displaying for the needs of the operator 800 the information contained in an electronic or any other form in the document source 200. The operator identifies and authenticates himself/herself through the security block 104.

The real time block 107 maintains the information on the real time required by the cryptographic operations needed for the generation of the crypto mark.

Another integral part of the document inspection block 500 is the crypto mark scanning block 501 which transforms the machine-readable crypto mark into the electronic form that is subsequently sent to the processor 502. The processor 502 carries out cryptographically the integrity verification and transmits the electronic form of the document 300 into the displaying block 506 where it will be made available to the operator 801 who has meanwhile authenticated himself/herself against the document inspection block 500 through the security block 505.

Based on the information collected from the electronic form of the document 300, on the data provided by the real time block 507, on the data regarding the location of the document control block 500, and on the data on operator 801 provided by the security block 505, the crypto stamp generation block 504 will generate a crypto stamp 900.

The operator 801 will affix the crypto stamp 900 to the inspected document 300 either manually according to information displayed on the displaying block 504 or, alternatively, via an automated equipment (printer) connected to the crypto stamp generation block 504.

Key generation and distribution block 700 performs a cryptographically safe generation of keys used in the cryptographic operations carried out within items 100, 500, and 600.

The key storage block 702 located within the key generation and distribution block stores the keys that are used for the needs of blocks 100, 500, and 600.

The key distribution blocks 701A and 701B perform - through communication with blocks 100, 500, and 600 - the distribution of the keys and their updating.

The key generation block 703 generates the crythographically safe keys.

The DB comparison block 600, which is shown in more detail in Figure 2, performs the comparison of individual items from two databases, i.e. from shadow DB 101 and feedback DB 503 sent into block 600 from block 500.

The comparison and evaluation proceeds within the block 601 according the appropriate comparison and evaluation criteria available from block 603. The results are entered into the alarm and warning block 602.

The statistics summary block 604 creates databases for the needs of higher statistical operations.

- 8-

Example 2

One of the preferred applications of the presented invention is its use for the protection of both customs documents and operations involving those documents.

Customs documents are generated in an electronic form to be subsequently converted into their printed versions on internationally standardized forms. At the places of their creation, the appropriate customs officials affix to the documents thus created their traditional stamps and signatures. The document contains less than 200 characters which form the critical information.

The invention enables the documents to be marked by a sticker carrying a crypto mark containing, besides the electronic signature with the secret key of the customs house where the document has been created, also the entire critical information characterizing the document, which is in an encrypted form. The crypto mark may be, for example, in the form of a complex bar code printed by a laser printer on a paper base (the sticker).

One copy of the document remains at the place of its generation, while the other copy (provided with the same sticker) is transferred by the party involved in the customs transaction (e.g. the importer or exporter) to the document control point (e.g. the customs house at the border crossing).

All data regarding the document and the customs officer are entered in an encrypted form into a shadow database and sent to a point where they will undergo comparison.

At the document control point, the inspecting authority scans the crypto mark by a laser scanner connected to a computer and the information it contains will be displayed on the screen. The critical parts of the documents thus displayed shall be compared with their counterparts which are in the printed form of the same document. Having performed the remaining operations of the customs proceedings (inspection of the cargo and verification of its intactness), the customs officer concludes the proceeding by entering the appropriate command into the computer.

The data will be entered in an encrypted form into a shadow database, this procedure will be followed by the displaying of a set of numerals representing the crypto stamp which will be written by the customs officer (by hand) onto the document that is being inspected.

Every customs officer (the operator), whether at the place of the creation of the document or at the document inspection point, proves to the computer his/her authorization to perform the required customs-related operation by the use of a special token (e.g. a special form of a chip card). The identity of the customs officer will be recorded in both databases (i.e. the shadow DB located at the place of creation of the document and the feedback DB located at the document inspection point).

The electronic signature is performed by an asymmetric cryptographic method ensuring the minimization of the danger of the loss of the key (i.e. in the case when the computer at the document control point is a portable hand-held bar code scanner with a built-in micro processor, a small displaying unit and a keyboard capable of the full scale generation of the crypto stamp).

The Center carries out the complex process of the item-matching process which is based on data extracted from both databases (shadow and feedback) and generates the warning/alarm messages for the appropriate customs authorities.

The crypto mark and or crypto stamp may be used successfully also in the number of other applications, e.g. in customs warehouses, in the handling of documents associated with the flow of goods to and from warehouses, etc.

The invention may be utilized also in the handling of the documentation and accompanying subsequent operations within large transport systems (cargo, air, rail, and road transport).

Industrial Applicability

A viability of the industrial applicability of the invention may by documented by its possible use in the areas of customs-related operations and logistical operations within large transportation system, as outlined in the above described examples.

Claims

1.   A system designed for the protection of documents and for preventing their unwarranted and unauthorized alteration and counterfeiting, enabling a falsification-proof confirmation of inspection-related operations, and minimizing the effect of the human factor. characterised in that consist of:

  — at least one document generation block (300) generating on the basis of document data source (200) and with the participation of an authenticated operator (800) a physical form of a document, a crypto mark (400) to be affixed onto that document, and a shadow database (101) for the storage of such documents;

  — at least· one document inspection block (500) performing the following functions: scanning of the crypto mark (400) borne by the document, verification of the authenticity of that document, display of the critical parts of the document and generation of a crypto stamp (900) to be affixed by either an authenticated operator (800) and/or (801) or by an appropriate equipment to the document, and generation of a feedback document database (503);

  — at least one key generation and distribution block (700);

  — at least one document database comparison block (600);

  — at least one document source block (200).

2.   A system as claimed in Claim 1, characterised in that the document generation block (101) consists of:

  — a processor (102) performing the processing of data and storing of the crypto keys;

  — a document printing block (105);

  — a crypto mark generating block (400);

  — a security block (104);

  — a real time block (107);

  — a displaying block (106); and

  — a shadow document database generation block (101).

3.   A system as claimed in Claim 1, characterised in that the document inspection block (500) consists of:

  — a processor (502) performing data processing and storing of the crypto keys ;

  — a block performing the scanning of the crypto mark (501);

  — a security block (505);

  — a real time block (507);

  — a displaying block (506);

  — feedback document database creating block (503); and

  — a crypto stamp generating block (504).

4.   A system as claimed in Claim 1, characterised in that the key generation and distribution block (700) consists of:

— a key generating block (703);

— a key storing block (702), and

— a key distribution block (701A) and/or (701B).

5.   A system as claimed in Claim 1, characterised in that the database comparison block (600) consists of:

— a comparison and evaluation block (601);

— a comparison criteria block (603);

— an alarm and warning generating block (603); and

— a statistics summary block (604).

6.   A method for the protection of documents and for preventing their unwarranted and unauthorized alteration and counterfeiting, enabling a falsification-proof confirmation of inspection-related operations, and minimizing the effect of the human factor, characterised in that consist of the following steps:

Cryptographic processing of selected data at the place of the generation of the document which serves as the source of data for the printout of that document, and conversion of the data into a form representing a basis for the generation of the crypto mark;

Generation of a crypto mark by the appropriate equipment after the transformation of the cryptographically pre-processed data; the crypto mark becomes unseparable component of the document that will thus become its carrier mediating its transfer to another location of use of the document;

Scanning of the crypto mark at the document inspection point and its transformation into a data format;

Verification through cryptographic methods of the integrity and authenticity of the data scanned from the crypto mark

Approval of the inspection of the document by an authenticated operator after the conclusion of the inspection and of all related operations;

Generation and displaying of a crypto stamp which links the inspected document unambiguously to the location of the document control point and to the authenticated operator;

Affixing of the crypto stamp to the inspected document for the purpose of its later processing either manually by the authenticated operator or by appropriate equipment.

7.   A method as claimed in Claim 6, characterised in that the following operations carried out at the place of the document generation: accumulation of all documents that have been generated, affixing to a set of such documents of an electronic signature, and encrypting and transmitting of such documents either individually or as a shadow database into the database comparison block.

8.   A method as claimed in Claim 6, characterised in that the following operations carried out at the document inspection point: accumulation of all documents that have undergone inspection, affixing to a set of such documents of their electronic signature, and encrypting and transmitting of such documents either individually or as a feedback database into the database comparison block.

9.   A method as claimed in Claim 6, characterised in that the generated crypto mark -- provided it is represented by an independent physical object e.g. a sticker, an appendix to a document, etc. - becomes permanently attached to the document.

10.   A method as claimed in Claim 6, characterised in that the generation of the crypto mark represents an integral part of the generation of the document and where it is generated by the same method as the document itself on the part of the carrier of that document designated for that purpose.

11.   A method as claimed in Claim 6, characterised in that the generation of the crypto mark is performed by its merging with either the text itself and/or with its graphic part or with the document print background.

12.   A method as claimed in Claims 7 to 8, characterised in that the database operations which are being carried out in the DB comparison block involve the contents of both shadow and feedback databases.

13.   A method as claimed in Claim 6, characterised in that the cryptographic generation of the crypto stamp in the document inspection block located at the document inspection point is carried out on the basis of data scanned from the crypto mark and data collected at the document inspection point itself.

14.   A method as claimed in Claims 6 and 13, characterised in that the crypto stamp becomes affixed to the document and and/or becomes connected with the document.

15.   A method as specified in item 6 where the key generation block performs the generation of the encryption and decryption keys and their transmitting by a protected channel through the key distribution block to the document generation and document inspection blocks.

16.   A method as claimed in Claim 6, characterised in that the operator performs through the security block the operations required to confirm his/her authorization to perform activities involving the document generation block.

17.   A method as claimed in Claim 6, characterised in that the operator performs through the security block the operations required to confirm his/her authorization to perform activities involving the document inspection block.

18.   A method as claimed in Claims 16 and 17, characterised in that the operator performs activities required to confirm his/her identity and authorization to perform activities involving the document generation and/or document inspection blocks.
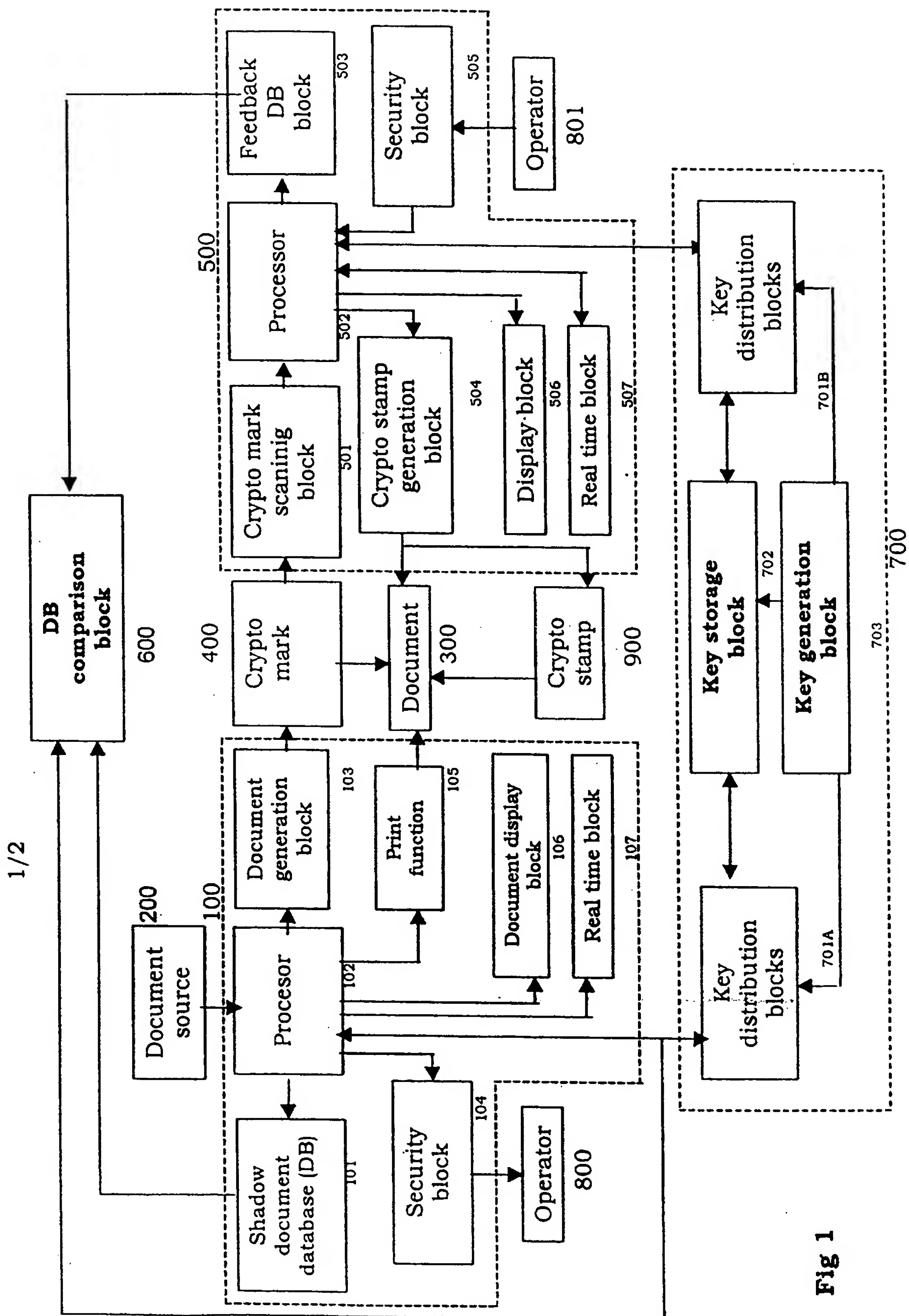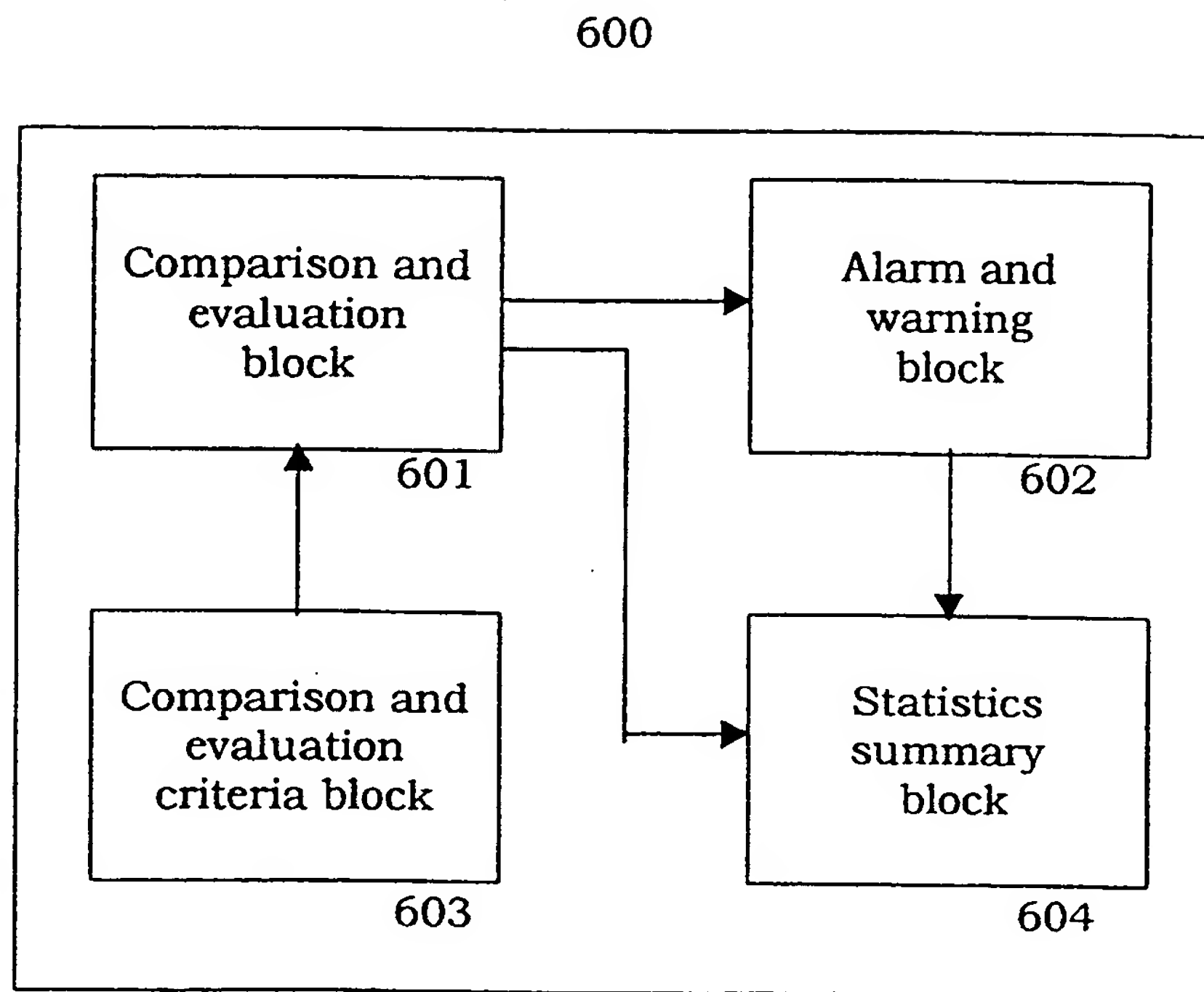
Fig 1

600

Fig. 2

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6   G07D7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6   G07D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 547 837 A (XEROX CORP) 23 June 1993 see claim 1; figure 1 ---	1-18
Y	US 5 388 158 A (BERSON WILLIAM) 7 February 1995 cited in the application see claim 1; figure 1 ---	1-18
A	EP 0 782 114 A (IBM) 2 July 1997 see claim 1; figure 1 ---	1-18
A	US 5 321 749 A (VIRGA RICHARD) 14 June 1994 cited in the application see claim 1; figure 1 --- -/--	1-18

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents. such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 February 1999	08/03/1999

| Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016 | Authorized officer

Kirsten, K |

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document. with indication.where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 530 755 A (PAILLES JEAN-CLAUDE ET AL) 25 June 1996 cited in the application see claim 1; figure 1 ─────	1-18

1

INTERNATIONAL SEARCH REPORT

..iformation on patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0547837	A	23-06-1993	US JP	5157726 A 6176036 A	20-10-1992 24-06-1994
US 5388158	A	07-02-1995	CA EP JP	2109554 A,C 0600646 A 7005809 A	21-05-1994 08-06-1994 10-01-1995
EP 0782114	A	02-07-1997	NONE		
US 5321749	A	14-06-1994	AU WO US	5135193 A 9407326 A 5398283 A	12-04-1994 31-03-1994 14-03-1995
US 5530755	A	25-06-1996	FR EP JP	2709218 A 0639919 A 7177278 A	24-02-1995 22-02-1995 14-07-1995